UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,277	03/06/2002	Ian Curry	10500.02.0123	7718

23418 7590 06/11/2007

VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
06/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/092,277	CURRY, IAN	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-28 are pending. Any well known statements made in the prior office action(s) not specifically and/or adequately traversed are taken as admittance of prior art as per MPEP 2144.03.

Response to Amendment and Arguments

Applicant's amendments and arguments were fully considered, but are moot in view of new rejections presented below that are made in response to the amendments. The 101 rejections made in the prior office action are withdrawn in light of applicant's amendments.

With respect to art rejections, applicant argues that Perlman does not teach encrypting a secret key using a corresponding public key specific to the intended recipient. The examiner respectfully disagrees. While it is true that Perlman does spend time discussing an embodiment of his invention in which a secret key, i.e. message key 210, is encrypted with a group secret key 314. It is not beyond the scope of his invention that a public key which corresponds to a specific intended recipient is used in place of group secret key 314 (see Fig 3 and col 5, lines 55-61). In fact, as seen in Figure 3, the encryption of the message/secret key could be accomplished using any of a recipient's public key 312, group secret key 314, ssl session key 316, or certificate public key 317 and the encrypted message/secret key is sent to the recipient who decrypts the encrypted message/secret key to obtain the message key 204. Column 5, lines 55-61 discusses use of a public key 312 that is specific to receiver 106. It should be appreciated that if a recipient's public key was used to encrypt the

message/secret key, then the recipient's private key would be utilized to decrypt the encrypted message/secret key.

Claim Objections

Claims 1, 15, 18, 20, and 24 are objected to because of the following informalities:

1. Claims 1, 15, 18, 20, and 24 were amended to recite "...public key specific to the intended recipient.... It is noted that earlier in these independent claims "at least one intended recipients" were recited, thus the examiner respectfully submits that applicant's amendments should have instead recited "...public key specific to the at least one intended recipients..." so as to be consistent with what was earlier recited in the claims or "...public key specific to at least one recipient..." so as to be consistent with the production of "at least one recipient specific secure secret key..." later recited in the claims. The examiner will reject the claims based on what it appears applicant has argued the meaning of the claims to be in the remarks submitted. It appears that applicant meant to state that each at least one intended recipient has their own public/private key pair that is specific to a single recipient and no other and the public key of each recipient is used to encrypt the decrypted secret key.
2. In lines 10-11 of claim 15, "of the recipient" should be deleted.
3. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-8, 10, 12, 15-24, and 28 are rejected under 35 U.S.C. 102(e) as being anticipated by Perlman et al (US 6,912,656).

Claim 1:

Perlman discloses the limitations of:

1. Receiving encrypted information, i.e. encrypted message 206 formed from encrypting message 105, from a sender for transmission to at least one intended recipient (col 5, lines 10-26) and receiving an encrypted secret key encrypted using a public key, i.e. public key 107, associated with a secure distribution server, i.e. DLE 110 and group server 114 (col 5, lines 28-31 and col 7, lines 41-59).
2. Decrypting the encrypted secret key to produce a decrypted secret key (Fig 4A-4C and col 7, lines 41-59).
3. Obtaining a corresponding public key, i.e. recipient public key 312, of the at least one intended recipient (Fig 3 and col 5, lines 55-61).

4. Encrypting the decrypted secret key for the at least one intended recipient using a corresponding public key specific to the at least one intended recipient to produce at least one recipient specific secure secret key, i.e. encrypted message key 308 (Fig 3; col 5, lines 55-61; Fig 4A-4C and col 7, lines 41-59).
5. Forwarding the encrypted information sent by the sender and at least one recipient specific secure secret key for the at least one intended recipient (Fig 3; Fig 4A-4C; col 5, lines 23-37; and col 7, lines 51-59).

Note that while Perlman does discuss his invention with respect to an embodiment of his invention in which a group secret key 314 is used to encrypt the message/secret key 204, Figure 3 shows that in his invention a recipient public key 312 could be used in place of group secret key 314. The recipient public key 312 is a corresponding public key specific to the at least one intended recipient 106.

Claim 2:

Perlman further discloses determining a plurality of intended recipients and retrieving corresponding public keys of the plurality of intended recipients for encrypting the decrypted secret key (Fig 3; Fig 4A-4C; and col 2, lines 22-31).

Clam 3:

Perlman further discloses encrypting a copy of the decrypted secret key for each intended recipient (col 7, lines 41-59) with a corresponding recipient public key (Fig 3 and col 5, lines 55-61).

Claim 4:

Perlman further discloses encrypting information with the secret key to produce the encrypted information, encrypting the secret key with a public key associated with the secure distribution server to produce the encrypted secret key, and sending the encrypted information and the encrypted secret key to the secure distribution server (Fig 4A-4C; col 5, lines 10-15 and 34-37; col 6, lines 47-65; and col 7, lines 41-59).

Claim 5:

Perlman further implicitly discloses wherein encrypting the secret key includes encrypting the secret key using a public key for each of a plurality of secure distribution servers to produce a plurality of secure distribution server specific encrypted secret keys (Fig 4A-4C and col 4, lines 47-51).

Claim 6:

The limitation of storing the encrypted information in an encrypted form locally on a device that performed the step of encrypting information with the secret key is inherent to Perlman's invention. To be able to encrypt and then forward the encrypted information to the secure distribution server, the device which performed the encryption process must store the encrypted information locally in memory before being able to send the encrypted information.

Claim 7:

Perlman further discloses the step of encrypting the secret key, by a sending device, with a public key associated with at least one of a user of the sending device and the sending device (Fig 3 and 4A-4C). Note that the DLE and group server are also sending devices. The recipients are users of the DLE and group server.

Claim 8:

Perlman further discloses the step of digitally signing the information using a private signing key associated with at least one of a user of a sending device and the sending device (col 4, lines 52-64 and col 5, lines 58-67).

Claim 10:

Perlman further discloses the step of determining, by the secure distribution server, if the encrypted information needs to be sent to other entities, if so, encrypting the decrypted secret key using a public key associated with each of the additional entities (Fig 4A-4C; col 5, lines 10-15 and 34-37; col 6, lines 47-65; and col 7, lines 41-59). Note the other entities read on the additional recipients in the distribution list.

Claim 12:

Perlman further discloses wherein retrieving the corresponding public keys of the plurality of intended recipients for encrypting the decrypted secret key includes obtaining the corresponding public keys from at least one of: a certificate retrieval and validation service, an LDAP lookup and a certificate directory lookup (col 7, lines 13-28).

Claim 15:

Perlman discloses the limitations of:

1. Receiving, by a secure distribution server, encrypted information from a sender for transmission to a plurality of recipients and an encrypted secret key encrypted using a public key associated with a secure distribution server (col 5, lines 28-31 and col 7, lines 41-59).

2. Decrypting, by the secure distribution server, the encrypted secret key to produce a decrypted secret key (Fig 4A-4C and col 7, lines 41-59).
3. Obtaining, by the secure distribution server, a corresponding public key of the at least one intended recipient (Fig 3 and col 5, lines 55-61).
4. Encrypting, by the secure distribution server, the decrypted secret key for the at least one intended recipient using a corresponding public key specific to the at least one intended recipient to produce a recipient specific secure secret key (Fig 3; col 5, lines 55-61; Fig 4A-4C and col 7, lines 41-59.
5. Forwarding, by the secure distribution server, the encryption information and the recipient specific secure secret key for a corresponding intended recipient (Fig 3; Fig 4A-4C; col 5, lines 23-37; and col 7, lines 51-59).

Claim 16:

Claim 16 recites a limitation substantially similar to what is recited in claim 2 and is rejected for the same reasons.

Claim 17:

Claim 17 recites a limitation substantially similar to what is recited in claim 3 and is rejected for the same reasons.

Claim 18:

Claim 18 is directed towards a network work element comprising one or more processing devices operative to implement the method of claim 1. Claim 18 is rejected for similar reasons given in claim 1.

Claim 19:

Claim 19 recites a limitation substantially similar to what is recited in claim 12 and is rejected for the same reasons given for claim 12.

Claim 20:

Claim 20 is directed towards a storage medium comprising memory containing executable instructions that when read by one or more processing devices, causes the one or more processing devices to implement the method of claim 1. Note that because Perlman's invention is computer implemented, a memory containing executable instructions that when read by one or more processing devices, cause the one or more processing devices to perform the method of claim 1 is inherent to Perlman's invention. Claim 20 is rejected for the same reasons given in claim 1.

Claim 21:

Claim 21 recites a limitation substantially similar to what was recited in claim 2 and is rejected for the same reasons.

Claim 22:

Perlman further inherently discloses memory containing executable instructions that when read by the one or more processing devices causes the one or more processing devices to encrypt a copy of the decrypted secret key for each intended recipient with a corresponding recipient public key (Fig 3 and 4A-4C).

Claim 23:

Perlman further inherently discloses memory containing executable instructions that when read by the one or more processing devices causes the one or more processing devices to determine if the encrypted information needs to be sent to other

entities, if so, encrypting the decrypted secret key using a public key associated with each of the additional entities (Fig 3 and 4A-4C).

Claim 24:

Perlman discloses the limitations of:

1. At least one sender that encrypts information with a secret key to produce encrypted information, encrypts the secret key with a public key associated with a network element to produce an encrypted secret key, and during an online session, sends the encrypted information and the encrypted secret key to the network elements (Fig 1, item 104 and 4A-4C).
2. At least one intended recipient (Fig 1, items 106 and 108).
3. At least one network element, operatively coupled to the sender and to the at least one intended recipient (Fig 1, items 110, 116, and 114), including one or more processing devices as recited in claim 18.

The one or more processing devices of the at least one network element recited in claim 24 are rejected for the same reasons given in claim 18.

Claim 26:

Claim 26 recites the network element performing the limitation of the method recited in claim 12 and is rejected for the same reasons given in claim 12.

Claim 28:

Claim 28 is directed towards at least one processing device including means for performing the decrypting, obtaining, and encrypting steps recited in claim 18 and is rejected for much the same reasons as claim 18.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 9, 13, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656).

Claim 9:

Perlman does not explicitly disclose the step of receiving the encrypted information and the encrypted secret key and forwarding the encrypted information and the encrypted secret key to the secure distribution server without decrypting the encrypted secret key. However, this limitation reads on forwarding/routing packets by nodes in a network, which the examiner take official notice as being was well known and commonly used in networks at the time applicant's invention was made. It would have been obvious to one of ordinary skill in the art to have modified Perlman's invention according to the limitations recited in claim 9. One of ordinary skill would have

been motivated to do so as direct connections between a sender and receiver in a network are rare and packets often have to be received and forwarded by other nodes in the network before the packets get to the final destination node.

Claim 13:

Perlman discloses the steps of: encrypting information with a secret key to produce the encrypted information, encrypting the secret key with a public key associated with the secure distribution server to produce the encrypted secret key, and during an online session, sending the encrypted information and the encrypted secret key to the secure distribution server (Fig 4A-4C).

Perlman does not explicitly disclose the encryption of the information and secret key are done offline. However, the examiner submits that encrypting information and a secret key offline was well known in the art. For example, it is well known that a user can prepare an email message for sending on a laptop when the laptop does not have a network connection, i.e. if the user was on a plane for a business trip. The message is usually prepared to a state where the only thing needed to be able to send the email is a network connection. Later, when the laptop is connected to a network, the message can then be sent. It would have been obvious to have the encryption of the message and key done offline prior to connecting to a network as the encryption process might take a long time and connection charges on the road can be expensive.

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Perlman's invention according to the limitations recited in claim 13. One of ordinary skill would have been

motivated to do so as it is common practice to be able to prepare messages offline during business trips and one of ordinary skill would have been motivated to encrypt the message and key offline prior to sending when a computer is online as it would reduce the amount of time the computer has to be connected to a network; this would reduce connection fees where the user is charged by the minute.

Claim 25:

Claim 25 recites a limitation substantially similar to what is recited in claim 13 and is rejected for the same reasons.

Claims 11 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656) in view of Chen et al (US 5,832,208).

Claim 11:

Perlman discloses the steps of: encrypting the decrypted secret key using a public key and sending the encrypted information and the encrypted secret key.

Perlman does not disclose the public key is associated with a content scanning device; the sending is to the content scanning device; receiving a result back from the content scanning device, forwarding the encrypted information based on the result sent by the content scanning device and based on at least one recipient specific secure secret key for at least one intended recipient.

However, Chen discloses a virus scanner, i.e. content scanning device, being implemented on a server (col 5, lines 53-60). Chen discloses that emails sent to the

server are scanned for viruses, an alert is generated if a virus is detected, and if possible, the virus is removed from the email attachment (col 5, lines 25-27 and col 7, lines 57-60).

In light of Chen's teachings, it would have been obvious to one of ordinary skill in the art to have combined Perlman and Chen's teachings according to the limitations recited in claim 11. One of ordinary skill would have been motivated to do so as scanning messages for viruses and removing the virus from email messages would prevent the spread of viruses to recipients of the email messages, which would compromise the recipient's system and any network they are attached to.

Claim 27:

Claim 27 recites a network element which performs the limitations of the method recited in claim 11 and is rejected for the same reasons given in claim 11.

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656) in view of Bouchard et al (US 2002/0091928).

Claim 14:

Perlman does not disclose sending the encrypted information to a time stamper and receiving a time stamped result prior to forwarding the encrypted information and the at least one recipient specific secure secret key to the at least one corresponding intended recipient.

However, Bouchard discloses time stamping a message by a time stamper prior to forwarding the message to a recipient (p3, paragraph 31, lines 11-15 and Fig 2). In light of Bouchard's teachings it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Perlman's invention according to the limitations recited in claim 14. One of ordinary skill would have been motivated to do so as Bouchard discloses that applying a time stamp to a message allow for an audit log of the message, which is useful in preventing the repudiation of digitally-signed documents/messages (p3, paragraph 28).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100